Abstract of the Disclosure

The present invention provides permutation instructions which can be used in software executed in a programmable processor for solving permutation problems in cryptography, multimedia and other applications. PPERM and PPERM3R instructions are defined to perform permutations by a sequence of instructions with each sequence specifying the position in the source for each bit in the destination. In the PPERM instruction bits in the destination register that change are updated and bits in the destination register that do not change are set to zero. In the PPERM3R instruction bits in the destination register that change are updated and bits in the destination register that do not change are copied from intermediate result of previous PPERM3R instructions. Both PPERM and PPERM3R instruction can individually do permutation with bit repetition. Both PPERM and PPERM3R instruction can individually do permutation of bits stored in more than one register. In an alternate embodiment, a GRP instruction is defined to perform permutations. The GRP instruction divides the initial sequence in the source register into two groups depending on control bits. The first group is combined with the second group to form an intermediate sequence toward the desired final permutation. The total number of GRP instructions for a bit level permutation of n bits is not greater than $\lg n$. The GRP instruction can be used to permute k-bit subwords packed into an n bits word, where k can be 1, 2, ..., or n bits, and $k*r = n$. At most $\lg r$ permutation instructions are used in the permutation instruction sequence, where r is the number of k-bit subwords to be permuted. The GRP instruction can also be used to permute $2n$ bits stored in two n-bit registers. The total number of instructions for bit permutation of $2n$ bits is $2\lg n+4$, and two of those instructions are SHIFT PAIR instruction.